

Example Company, Inc.
Identity Management Architecture
Policy on Authentication

Status: [Approved | Draft – RFC | Final Draft – Awaiting Approval]

Date: 01APR04

1.0 Purpose

The purpose of this policy is to provide guidance concerning user authentication on information systems at Example Company, Inc..

2.0 Scope

This policy applies to all Example Company, Inc. projects, procurements, employees and affiliates.

3.0 Definitions

4.0 References

Policy on Naming and Certificates
Policy on Passwords
Policy on Directories
Policy on Access Control

5.0 Policy

5.1 Use of Enterprise Directory. The enterprise directory shall be used as the user authentication database for access to all Example Company, Inc. information systems where access control is required, unless the information system in question is not technically capable of interfacing to the enterprise directory. Exceptions require written approval from the Office of the CIO.

5.2 User IDs. User IDs shall be the unique ID created by the Policy on Naming and Certificates.

5.3 Selecting Authentication Systems. Compatibility with enterprise directory shall be required when specifying or selecting authentication systems. Exceptions require written approval from the Office of the CIO. Whenever an information system undergoes major modification, the project management shall determine whether the system should be brought into compliance with this policy and justify their decision to the Office of the CIO.

5.4 User Accounts. Unless it is technically unavoidable, user accounts shall not be shared by more than one individual. Where it is technically unavoidable, other mechanisms shall be implemented to provide individual traceability.

5.5 Authentication Levels. The following authentication levels are defined:

- Casual – no password is required. A simple token such as a cookie is used to establish identity.
- Standard – standard ID and password combination shall be required.
- Secure – a physical token shall be required in addition to ID and password.
- Critical – a separate ID and password (different than those used to authenticate to access to less secure systems) shall be required in addition to a physical token.

Biometric, digital certificates and other techniques may be used in addition to these at the discretion of the system architect. Substitution of authentication mechanisms for any given level must be approved in writing by the Office of the CIO.

5.6 Authentication Audits. The Chief Security Office is responsible for auditing authentication systems and processes. Processes will be audited once per year. Information systems will be audited in the design phase, as part of the pre-launch quality assurance process, and after any major system upgrades.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Contacts

7.1 Custodian

IMA Team, Office of the CIO
imateam@example.com
801.555.1212 x563

7.2 Approval Body

Identity Management Architecture Review Board

8.0 Revision History

Version	Approval Date	Comments
1.0	01APR04	Initial version approved.